Hommage an Wireshark

Warum das Schweizer Taschenmesser Wireshark nicht mehr ausreicht …und was man stattdessen tun kann!

Wireshark ist ein fantastisches Expertenwerkzeug für die tiefgehende Fehlerbehebung auf Paketebene!

Moderne Automobilnetzwerke, zonale E/E-Architekturen und softwaredefinierte Fahrzeuge (SDV) sind jedoch echtzeitfähig, sicherheitskritisch und zeitgesteuert.

Bei ihrer Validierung geht es nicht mehr nur um die Frage „Kann ich diesen Frame decodieren?“, sondern auch darum zu ergründen „Erfüllt jeder zeitkritische Datenstrom seine Latenz-/Jitter-/Zuverlässigkeitsgarantien unter Last und bei Fehlern im gesamten Fahrzeug?“

Diese Aufgabe erfordert schnelle, hoch belastbare, zeitlich synchronisierbare, multipunktfähige, streambewusste und standardkonforme Tools.

Moderne Validierungstools MÜSSEN dies leisten können; Wireshark kann dies nicht.

Was hat sich geändert?

Von „Paketen auf einem Bus“ zu „Echtzeit-verteilten Systemen“

Die Validierung erfordert nun den Nachweis auf Systemebene, dass diese Garantien durchgehend und über einen längeren Zeitraum hinweg eingehalten werden, und nicht nur den Nachweis, dass ein Paket angekommen ist. Dies muss sowohl über alle Verbindungen hinweg, als auch während der gesamten Zeit, in der das Paket „auf der Leitung“ ist, erfolgen und korreliert werden.

Zonal-/SDV-Netzwerke kombinieren:

- Time-Sensitive Networking (TSN)-Funktionen (802.1AS/gPTP, Qbv TAS, Qav/CBS, Qcc, Qci PSFP, Qbu/Qbv-Präemption, 802.1CB FRER usw.)
- Verkehr mit gemischter Kritikalität (Regelkreise, Sensorik, Diagnose, Over-the-Air-Updates, Infotainment)
- Serviceorientierte Stacks (SOME/IP, DoIP) auf deterministischem Ethernet
- Harte Zeitlimits (z. B. <2 ms E2E für die Steuerung; <50 µs Hop-Latenzabweichung; hohe Verfügbarkeit), Legacy-CAN, A²B-Kommunikation – alles miteinander korreliert!

Das (Daten-)Problem, über das man ungern spricht:

Moderne Fahrzeuge generieren *riesige* Datenmengen: Multi-Gigabit-Ethernet-Backbones, Dutzende von Kameras/Sensoren, kontinuierliche Protokollierung und OTA-/Services. Wireshark eignet sich hervorragend für die interaktive Debugging auf Paketebene bei *Megabyte- bis Gigabyte-Captures* –ist aber nicht auf *Dutzende oder gar Hunderte* von Gigabytes und schon garnicht auf Terabytes skalierbar. Hier ist der Grund dafür:

Die einfache, brutale Mathematik auf durchschnittlichen PCs

- Öffnungs-/Vorbereitungsgeschwindigkeit von Wireshark: dauert ~ 20 s pro GB
- Zeitkosten eines einfachen Filters: × 1,7 (≈ +70 % Zeitaufwand zusätzlich)

Durchschnittliche Zeit, die Wireshark zum Öffnen von Dateien benötigt*

(Dies gilt nur für das Öffnen, NICHT für die Analyse!

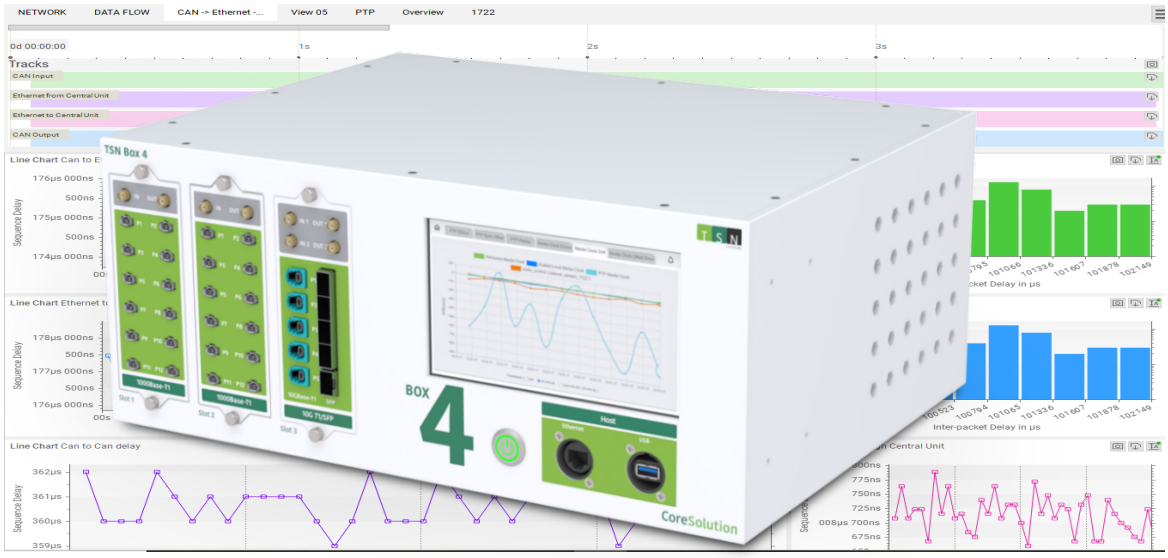
Dateigrößen	Nur öffnen (20 s/GB)	Mit 1 einfachen Filter (×1,7)
500 GB	2 Std. 46 Min.	4 h 43 m
1 TB (1000 GB)	5 Std. 33 Min.	9 Std. 27 Min.
4-min Capture bei (~3 GB/s ≈ 720 GB)	4 Std. 00 Min.	6 Std. 48 Min

Diese Zeiten beziehen sich nur auf die Erfassung/Indizierung von Daten. Die Zahlen beschreiben Beispiele für Datentraces in der SDV-Validierung. *Jede Anpassung eines Filters oder jede Änderung der Ansicht wiederholt während der Analyse große Teile dieses Aufwands.*

**Weitere Einblicke finden Sie in dem Artikel “Warum Wireshark unter der Last moderner Fahrzeugdatenmengen zusammenbricht”, der ebenfalls auf https://tsn.systems/downloads/#c1027 veröffentlicht wurde.*

TSN Systems CoreSolution 4

Speziell entwickelte moderne Toolchain zur Verarbeitung datenintensiver Zonenarchitektur und SDV-Validierung



- Integrierte Analyse und Filterung (destruktiv und nicht-destruktiv)
- **Alle** Taps sind direkt an den superschnellen internen **2-Terabit/s**-PCIe-Bus angeschlossen
- **Alle** Taps **sind direkt mit internen Multi-Terabyte-Hochgeschwindigkeits-SSDs verbunden**
- **Echtzeitverarbeitung** und **Echtzeitanalyse** sind während und nach der Aufzeichnung/Erfassung von Daten verfügbar
- **Projektdateien mit einer Größe von mehreren Terabyte** können **sofort** überprüft und analysiert werden
- Alle **Filtereinstellungen** oder Änderungen in Analysern können quasi sofort vorgenommen werden und erfordern KEINE zeitaufwändigen erneuten Datenscans des gesamten Traces
- **Die Größe der Projektdatei** ist nur durch die Anzahl und Größe der integrierten SSDs begrenzt
- Jeder moderne PC mit einer Gigabit-Ethernet-Schnittstelle kann angeschlossen werden und die TSN **CoreSolution Analyser-Software** ausführen
- **Bis zu 36 x 1 Gb (18 Taps)** und/oder **bis zu 10 x 10 Gb (4 Taps) T1- oder T-Ports** können gleichzeitig verwendet werden.

Wireshark vs. CoreSolution 4 Fact Sheet

	Gigabyte	Ladezeit (s)	Filterkanal	Zeit (s)	Zeit (h)	Tests	Zeit Mh	Zeit MM	Kosten EU**	Kosten Welt***
Wireshark	25	500	4	3400	2	100	194	1.22	12 056	4861
CoreSolution	25	1	4	6.8	1	100	100	0.63	6 212	2505
Wireshark	250	5 000	4	34 000	10	100	1044	6.53	64 756	26 111
CoreSolution	250	1	4	6.8	1	100	100	0.63	6212	7013
Wireshark	1 000	20 000	4	136 000	39	100	3878	24.24	240 422	96944
CoreSolution	1 000	1	4	6.8	1	100	100	0.63	6212	2505

Die Tabelle vergleicht die Verarbeitungszeiten von Wireshark und TSN CoreSolution in 100 Tests mit Dateigrößen von 25 GB, 250 GB und 1 TB.

Jeder Test geht von vier Filteränderungen plus einer Stunde Analysezeit aus.

Mit zunehmender Dateigröße wächst der Zeitunterschied in etwa linear:

* Bei 25 GB benötigt Wireshark mehr als doppelt so lange wie CoreSolution.
  (Wenn eine stärkere Filterung erforderlich ist – z. B. 12 Filter pro Test – verdoppelt sich der Faktor nochmal fast auf ~4.)

* Bei 250 GB steigt der Faktor auf **das Zehnfache der benötigten Zeit.**

* Bei 1 TB vergrößert **sich** der Abstand auf **das 40-fache.**

Hier bewerten ausschließlich den Zeitfaktor.
Und das ist kein reines Wireshark-Problem—es betrifft die große Mehrheit aller Testsysteme und Toolchains gleichermaßen, da die große Mehrheit davon das gleiche Monolithische Dateidenken wie Wireshark ihrer Analyse zugrunde legt.

Die Zeitersparnis durch die zusätzlichen Analysemöglichkeiten der TSN CoreSolution wird dabei NICHT berücksichtigt!

Wenn Sie mehr über andere Aspekte als den Zeitaufwand erfahren möchten, finden Sie weitere Informationen in dem Artikel " Warum Wireshark unter der Last moderner Fahrzeugdatenmengen zusammenbricht", der ebenfalls auf veröffentlicht ist.

** Die Kosten werden auf der Grundlage von 62 € pro Ingenieur (VDA) berechnet.

***Die Kosten werden auf der Grundlage von 25 € pro Ingenieur berechnet